UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,562	10/28/2005	Takehiko Nakano	266812US6PCT	6309

22850 7590 02/19/2009

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
SHOLEMAN, ABU S	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
02/19/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/528,562	NAKANO ET AL.	
	Examiner	Art Unit	
	ABU SHOLEMAN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-14,16-19,21-23,25 and 26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-14,16-19,21-23 and 25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/03/2008, 06/14/2006, 02/09/2006,10/06/2005,03/21/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

1. Claims 1-4, 6-14, 16-19, 21-23, 25-26 of the instant application filed on 10/28/2005 are presented for examination.

Claim Objections

2. Claims 4,14,19,23 recites the limitation "Computer program product" in 1. There is insufficient antecedent basis for this limitation in those claims. Applicant did not disclose “computer program product” in the specification but it discloses “program”. So examiner is considering it as a software program.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 2 recites the limitation "a maximum of N times" in line 3. There is indefinite for this limitation in the claim because N does not belong to any limited number such as (N=1, 2, 3....).

5. Claims 9, 10, 11 recite the limitation "N times and N sets" in line 3 and line 7 respectively. There is indefinite for this limitation in the claim because N does not belong to any limited number such as (N=1, 2, 3....).

6. Claim 4 recites the limitation "the response request command" in line 5. There is insufficient antecedent basis for this limitation in the claim.

7. Claim 16 recites the limitation "said information receiving apparatus" in 12. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 4, 14, 19 and 23 are directed to a "computer program product". The computer program is not claimed as being stored on a tangible computer readable medium. As such, the above claims are simply a computer program product which could be a software and thus do not clearly establish a statuary category of the invention. They are, at best, functional descriptive material.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-4, 6-14, 16-19, 21-23 and 25-26 are rejected under 35 U.S.C 103(a) as being unpatentable over Haverinen et al (US 2002/0012433) (hereinafter Haverinen) in view of Rofheart et al (US 7058414) (hereinafter Rofheart).

As per claim 1, Haverinen discloses " a data transmitting apparatus " as (paragraph , 0174, discloses a GAGW GSM authentication gateway) comprising: "a

command transmission transmitting unit configured to transmit a response request command to a data receiving apparatus" as (paragraph 0061, sending a challenge to a mobile node) ; "a control unit configure to receive a response message to the response request command from the data receiving apparatus" as (paragraph 0062, receiving a first response from the mobile node)," the response message including authentication data based on shared data shared with said data receiving apparatus" as (paragraph 0055, a first response corresponding to the challenge , based on the shared secret); "an expected value generation unit configured to generate an expected authentication value based on the shared data" as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret); "an authentication unit configured to produce an authentication result for said data receiving apparatus based on the expected value and said authentication data" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data). **But Haverinen expressly fails to disclose** "a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message; and a judgment whether unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time".

However Rofheart discloses "a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message" as (Fig 7, compute round Trip time from transmitter to receiver); "and a judgment whether unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time" as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide secure enablement communication with a specific subscriber .

As per claim 2, Haverinen discloses " wherein: said command transmission unit is further configured to transmit said response request command a maximum of N times" as (paragraph 0038, challenge is n random for n session key) ; "said control unit is further configured to receive the response messages from the data receiving apparatus for each of the N transmitted response request commands" as (paragraph 0056, sending a response for each packet data); and "said authentication unit is further configured to produce authentication results based on said authentication data in each

received response message" as (paragraph 0099, verifying the first response to authentication at the mobile node) .

As per claim 3, Haverinen discloses "a data transmission method comprising: transmitting a response request command to a data receiving apparatus" as (paragraph 0061, GSM sending a challenge to a mobile node) ; "receiving a response message to the response request command from the data receiving apparatus" as (paragraph 0062, receiving a first response from the mobile node), "the response message including authentication data based on shared data shared with said data receiving apparatus" as (paragraph 0055, a first response corresponding to the challenge, based on the shared secret) ; "generating an expected authentication value based on the shared data" as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret) ; "producing an authentication result for said data receiving apparatus based on the expected authentication value and said authentication data" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data). **But Haverinen expressly fails to disclose** "measuring a response time between transmitting the response request command and receiving the response message; and "judging if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time".

However, Rofheart discloses “measuring a response time between transmitting the response request command and receiving the response message” as (Fig 7, compute round Trip time from transmitter to receiver); and “judging if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time” as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide secure enablement communication with a specific subscriber .

As per claim 4, Haverinen discloses “A computer program product having computer program instructions which when executed by a computer” as (paragraph o117, computer program executed by computer); cause the computer to perform the following steps: “controlling transmission of a command to a data receiving apparatus” as (paragraph 0061, GSM sending a challenge to a mobile node); “controlling reception of a response message to the response request command from the data receiving apparatus” as (paragraph 0062, receiving a first response from the mobile node), “the response message including authentication data based on shared data shared with said data receiving apparatus” as (paragraph 0055, a first response corresponding to

the challenge , based on the shared secret) ; "controlling generation of an expected authentication value based on the shared data" as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret) ; "controlling production of an authentication of result for said data receiving apparatus based on the expected authentication value and said authentication data" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data). **But Haverinen expressly fails to disclose** " controlling measurement of a response time between transmitting the response request command and receiving the response message; and "judging if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time".

However Rofheart discloses "controlling measurement of a response time between transmitting the response request command and receiving the response message" as (Fig 7, compute round Trip time from transmitter to receiver); and "judging if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time" as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide secure enablement communication with a specific subscriber .

As per claim 6, Haverinen discloses " an authentication data generation unit configured to generate said authentication data based on shared data shared with the data transmitting apparatus by subjecting said shared data to a predetermined process before said response request command is received from said data transmitting apparatus" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data); "a response message generation unit configured to generate the response message to said response request command before said response request command is received from said data transmitting apparatus" as(0062, receiving a first response from the mobile node), "said response message including said authentication data" as (paragraph 0055, a first response corresponding to the challenge , based on the shared secret) and "a transmission unit configured to transmit said response message to said data transmitting apparatus when said response request command is received from said data transmitting apparatus" as (paragraph 0109,the subscriber received the challenge and responsively to form a first response based on the challenge and the shared secret). **But Haverinen expressly fails to disclose** "A data receiving apparatus with

configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on authentication data and response time between sending a response request command and receiving a response message, the data receiving apparatus comprising: “a command receiving unit configured to receive the response request command from the data transmitting apparatus.

However Rofheart discloses “A data receiving apparatus with configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on authentication data and response time between sending a response request command and receiving a response message” as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response), the data receiving apparatus comprising: “a command receiving unit configured to receive the response request command from the data transmitting apparatus” as (column 3, line 61-65, transmitting a message from a local device to a remote device);

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide a sender can efficiently determined secure data transmission in a short time.

As per claim 7,Haverinen discloses “ wherein: said shared data is a quasi random number” as (paragraph 0037, the challenge are random); “transmitted from

said data transmitting apparatus before said response request command is transmitted" as (claim 0170, the challenge sent before response are received from the SIM); and" said authentication data generation Unit is further configured to subject said quasi random number to a Keyed-Hash process to produce a Hash value that is used as said authentication data " as (paragraph 0180 and Fig 2, hash value is calculated from random value in the authentication unit).

As per claim 8, Haverinen discloses "wherein: said authentication data generation unit is further configured to execute a Keyed-Hash process relative to said quasi random number and information specific to the information processing apparatus to produce a Hash value that is used as said authentication data" as (paragraph 0187 and Fig 2, authentication is complete and the FAAA and the MT share k and K is calculated by hashing the random).

As per claim 9,Haverinen discloses " that wherein: said command receiving unit is further configured to receive said response request command from said data transmitting apparatus a maximum of N times" as (Fig 2, N times of command are transmitted from MT to PAC); said" authentication data generation unit is further configured to execute said predetermined process relative to said shared data before a first one of said response request command commands is received from said data transmitting apparatus and further configured to generate N sets of said authentication data corresponding to said N received response request Commands" as (Fig 2, authentication is done on shared data. Each packet gets authenticated in each session);

and "said transmission unit is further configured to transmit said response message generated by said response message generation unit to said data transmitting apparatus, said response message including the N sets of said authentication data in a sequence agreed beforehand with said data transmitting apparatus" as (Fig 2. PAC sends response of N number of N packet data to MT after authentication).

As per claim 10, Haverinen discloses "wherein: said authentication data generation unit is further configured to divide the data obtained by subjecting said shared data to said process into a plurality of data pieces and further configured to generate the N sets of said authentication data from the divided data" as (Fig 2, it is obvious that packet data is division of whole data. GAGW authenticate each packet of data).

As per claim 11, Haverinen discloses: "wherein: said authentication data generation means unit is further configured to generate the N sets of said authentication data based on data obtained at each process of repetitively executing said predetermined process relative to said shared data" as (Fig 2, GAGW authenticate to the sequence of the packet data) .

As per claim 12, Haverinen discloses wherein: said transmission unit is further configured to transmit the response message to said transmitting apparatus when said response request command is received from the data transmitting apparatus, said response message containing new authentication data generated from said authentication data and information contained in said response request command" as (

Fig 2, GAGW transmits authentication information to PAC. When GAGW send response to PAC, Each authenticated data with the new authentication key).

As per claim 13, However Haverinen discloses " generating said authentication data based on shared data shared with the data transmitting apparatus by subjecting said shared data to a predetermined process before said response request command is received from said data transmitting apparatus" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data); "generating the response message to said response request command before said response request command is received from said data transmitting apparatus" as(0062, receiving a first response from the mobile node), "said response message including said authentication data" as (paragraph 0055, a first response corresponding to the challenge , based on the shared secret) and "a transmitting said response message to said data transmitting apparatus when said response request command is received from said data transmitting apparatus" as (paragraph 0109,the subscriber received the challenge and responsively to form a first response based on the challenge and the shared secret). **But Haverinen expressly fails to disclose** "A data reception method for data receiving apparatus configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on authentication data and a response time between sending a response request

command and receiving a response message, the data receiving method by comprising: receiving the response request command from the data transmitting apparatus".

However Rofheart "A data reception method for data receiving apparatus configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on authentication data and a response time between sending a response request command and receiving a response message" as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response), the data receiving method by comprising: " receiving the response request command from the data transmitting apparatus" as (column 3, line 61-65, transmitting a message from a local device to a remote device);

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide a sender can efficiently determined secure data transmission in short time.

As per claim 14, Haverinen discloses " controlling generation of said authentication data based on shared data shared with the data transmitting apparatus by subjecting said shared data to a predetermined process before said response

request command is received from said data transmitting apparatus" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data);" controlling generation of the response message to said response request command before said response request command is received from said data transmitting apparatus" as(0062, receiving a first response from the mobile node), "said response message including said authentication data" as (paragraph 0055, a first response corresponding to the challenge , based on the shared secret) and " controlling transmission of said response message to said data transmitting apparatus when said response request command is received from said data transmitting apparatus" as (paragraph 0109,the subscriber received the challenge and responsively to form a first response based on the challenge and the shared secret). **But Haverinen expressly fails to disclose** "A computer program product having computer program instructions which, when executed by a computer configured to receive data from a data transmitting apparatus which judges whether data transmission is granted, based on authentication data and a response time between sending a response request command and receiving a response message, causes the computer to perform the following steps: controlling the reception of the response request command from the data transmitting apparatus" .

However Rofheart discloses "A computer program product having computer program instructions which, when executed by a computer configured to receive data

from a data transmitting apparatus which judges whether data transmission is granted, based on authentication data and a response time between sending a response request command and receiving a response message" as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response), causes the computer to perform the following steps: " controlling the reception of the response request command from the data transmitting apparatus" as (column 3, line 61-65, transmitting a message from a local device to a remote device);

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide a sender can efficiently determined secure data transmission in a short time.

As per claim 16, Haverinen discloses " a information transmitting apparatus " as (paragraph , 0174, discloses a data transmission) comprising:" an authentication data generation means unit configured to generate command authentication data and response expected value data from shared data shared with a data receiving apparatus" as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value

from challenges value with shared secret); “a command transmission unit configured to transmit a response request command to a data receiving apparatus” as (paragraph 0061, GSM sending a challenge to a mobile node), “ the response message including authentication data based on shared data shared with said data receiving apparatus” as (paragraph 0055, a first response corresponding to the challenge , based on the shared secret); “a response reception unit configured to receive a response message to said response request command from the data receiving apparatus” as (paragraph 0062, receiving a first response from the mobile node); “an authentication unit configured to produce an authentication result for said information receiving apparatus based on said response expected value data and said response authentication data in said response message received from said data receiving apparatus” as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data). **But Haverinen expressly fails to disclose** “a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message; and a judgment means unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time”.

However Rofheart discloses “a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message” as (Fig 7, compute round Trip time from transmitter to receiver); “and a judgment means unit configured to judge if a subsequent data transmission to

said data receiving apparatus is granted based on the authentication result and the response time" as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide secure enablement communication with a specific subscriber .

As per claim 17, Haverinen discloses " wherein: said command transmission unit is further configured to transmit said response request command a maximum of N times granted " as (paragraph 0038, challenge is n random for n session key) ; "said control unit is further configured to receive the response messages from the data receiving apparatus for each of the N transmitted response request commands" as (paragraph 0056, sending a response for each packet data); and "said authentication unit is further configured to produce authentication results based on said authentication data in each received response message" as (paragraph 0099, verifying the first response to authentication at the mobile node).

As per claim 18, Haverinen discloses " a data transmission method characterized by " as (paragraph , 0174, discloses a data transmission) comprising:" generating command authentication data and response expected value data from shared data shared with a data receiving apparatus" as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret); " transmitting a response request command to said data receiving apparatus" as (paragraph 0061, GSM sending a challenge to a mobile node), " said response request command containing said authentication data " as (paragraph 0055, a first response corresponding to the challenge , based on the shared secret) ; " receiving a response message to said response request command from the data receiving apparatus" as (paragraph 0062, receiving a first response from the mobile node); "producing an authentication result for said information receiving apparatus based on said response expected value data and said response authentication data in said response message received from said data receiving apparatus" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data).**But Haverinen expressly fails to disclose** " measuring a response time between transmitting the response request command and receiving the response message; and judging if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time".

However Rofheart discloses “measuring a response time between transmitting the response request command and receiving the response message” as (Fig 7, compute round Trip time from transmitter to receiver); “and judging if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time” as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide secure enablement communication with a specific subscriber .

As per claim 19, Haverinen discloses " a computer program instructions which when executed by a computer ; cause the computer to perform the following steps:" as (paragraph , 0174, discloses a data transmission) comprising:” generating command authentication data and response expected value data from shared data shared with a data receiving apparatus” as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret);“ transmitting a response request command to said data receiving apparatus” as (paragraph 0061,

GSM sending a challenge to a mobile node), " said response request command containing said authentication data "as (paragraph 0055, a first response corresponding to the challenge , based on the shared secret); " receiving a response message to said response request command from the data receiving apparatus" as (paragraph 0062, receiving a first response from the mobile node); "producing an authentication result for said information receiving apparatus based on said response expected value data and said response authentication data in said response message received from said data receiving apparatus" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data).**But Haverinen expressly fails to disclose** " measuring a response time between transmitting the response request command and receiving the response message; and judging, if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time".

However Rofheart discloses "measuring a response time between transmitting the response request command and receiving the response message" as (Fig 7, compute round Trip time from transmitter to receiver); "and judging, If a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time" as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide secure enablement communication with a specific subscriber .

As per claim 21, Haverinen discloses "the data receiving apparatus comprising: a generating unit configured to generate command expected value data and response authentication data from shared data shared with said data transmitting apparatus" as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret) , "each of said command expected value data and said response authentication data corresponding to authentication data in said response request command generated at said data transmitting apparatus from said shared data" as (Fig 2, calculated value k and SIGNrand are related to random challenge sent from transmitter) ; "authenticating unit configured to produce an authentication result for said data transmitting apparatus based on the authentication data in said response request command and said command expected value data when said response request command is received from said data transmitting apparatus" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data) ; and "a transmission unit configured to transmit a subsequent response message containing said response authentication data

to said data transmitting apparatus based on the authentication result by said authenticating unit" as [Fig 11a , Send response to the MT after authentication process at (511)]. **But Haverinen fails to expressly disclose** "A data receiving apparatus configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on a response time between sending a response request command and receiving a response message".

However Rofheart discloses " A data receiving apparatus configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on a response time between sending a response request command and receiving a response message" as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide a sender can efficiently determined secure data transmission in a short time.

As per claim 22, Haverinen discloses, the method comprising: "generating command expected value data and response authentication data from shared data shared with said data transmitting apparatus" as (paragraph 0055, generating a

session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret) , “each of said command expected value data and said response authentication data corresponding to authentication data in said response request command generated at said data transmitting apparatus from said shared data’ as (Fig 2, calculated value k and SIGNrand are related to random challenge sent from transmitter) ; “producing an authentication result for said data transmitting apparatus based on the authentication data said in said response request command and said command expected value data when said response request command is received from said data transmitting apparatus” as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data) and “transmitting a subsequent response message containing said response authentication data to said data transmitting apparatus, based on the authentication result” as [Fig 11a , Send response to the MT after authentication process at (511)]. But Haverinen expressly fails to disclose “a data reception method for a data receiving apparatus configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on a response time between sending a response request command and receiving a response message”.

However Rofheart discloses “a data reception method for a data receiving apparatus configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on a response time between sending a

response request command and receiving a response message" as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide a sender can efficiently determined secure data transmission in a short time.

As per claim 23, Haverinen discloses, " generating command expected value data and response authentication data from shared data shared with said data transmitting apparatus" as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret) , "each of said command expected value data and said response authentication data corresponding to authentication data in said response request command generated at said data transmitting apparatus from said shared data " as (Fig 2, calculated value k and SIGNrand are related to random challenge sent from transmitter); "producing an authentication result for said data transmitting apparatus based on the authentication data in said response request command and said command expected value data when said response request command is received from said data transmitting apparatus " as (paragraph 0059, obtaining authentication information, the authentication information

unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data) ; and “transmitting a subsequent response message containing said response authentication data to said data transmitting apparatus based on the authentication result" as [Fig 11a , Send response to the MT after authentication process at (511)]. **But Haverinen expressly fails to disclose** “ A computer program product having computer program instructions which, when executed by a computer configured to receive data from a data transmitting apparatus which judges whether data transmission data is granted based on a response time between sending a response request command and receiving a response message.

However Rofheart discloses "A computer program product having computer program instructions which(it is obvious that method for the anonymous authentication of a data transmitter of computer program), “when executed by a computer configured to receive data from a data transmitting apparatus which judges whether data transmission data is granted based on a response time between sending a response request command and receiving a response message” as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a

device authentication with response time that taught by Rofheart because it would provide a sender can efficiently determined secure data transmission in a short time.

As per claim 25, However Haverinen discloses “an authentication data generation unit configured to generate said authentication data based on the shared data by subjecting said shared data to a predetermined process before said response request command is received from said data transmitting apparatus” as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data), “a response message generation unit configured to generate the response message to said response request command before said response request command is received from said data transmitting apparatus , said response message including said authentication data” as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret), and ” a transmission unit configured to transmit said response message to said data transmitting apparatus when said response request command is received from said data transmitting apparatus” as (Fig 2, PAC transmits a response message to MT after registration request). **But Haverinen expressly fails to disclose** “A communication system comprising “a data transmitting apparatus including, a command transmission unit configured to transmit a response request command to a data receiving apparatus, a control unit configure to receive a response message to the

response request command from the data receiving apparatus, a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message, and a judgment unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time the data receiving apparatus configured to receive data from the data transmitting apparatus, the data receiving apparatus including a command receiving unit configured to receive the response request command from the data transmitting apparatus.

However Rofheart discloses “A communication system comprising” as (Abstract ,communication system): “a data transmitting apparatus including” as (Fig 1A, Transmitting apparatus), “a command transmission unit configured to transmit a response request command to a data receiving apparatus” as (Fig 1A, Transmitter send data to the receiver), “a control unit configure to receive a response message to the response request command from the data receiving apparatus” as (Fig 1A, Transmitter received a response through controller) , “a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message” as (Fig 1A , response time is measured by timing generator), and “a judgment unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time” as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response). “The data receiving apparatus configured to receive data from the data transmitting apparatus” as (Fig 1A, Receiver apparatus

received data from transmitter), “the data receiving apparatus including” as (Fig1A, Receiver apparatus), “a command receiving unit configured to receive the response request command from the data transmitting apparatus” as (Fig 1A, Receiver gets data from transmitter).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that taught by Rofheart because it would provide a sender can efficiently determined secure data transmission in a short time.

As per claim 26, Haverinen disclose “ a communication system” as (Abstract : telecommunication network) comprising: “an information transmitting apparatus” as (Fig 2, information transmitting) including “an authentication data generation unit configured to generate command authentication data and response expected value data from shared data shared with a data receiving apparatus” as (Fig 2, request for authentication with random challenge to receiving apparatus), “a command transmission unit configured to transmit a response request command to said data receiving apparatus” as (Fig 2, MT send data to PAC for registration reply), “said response request command containing said command authentication data” as (Fig 2, random challenge data for authentication),“a response reception unit configured to receive a response message to said response request command from said data

receiving apparatus" as (Fig 2, MT received a reply massage from PAC),"an authentication unit configured to produce an authentication result for said information receiving apparatus based on said response expected value data and response authentication data in said response message received from said data receiving apparatus" as (Fig 2,paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret). "the data receiving apparatus" as (Fig 2, MT received data) including "a generating unit configured to generate command expected value data and the response authentication data from the shared data, each of said command expected value data and said response authentication data corresponding to the command authentication data in said response request command generated at said data transmitting apparatus from said shared data" as (paragraph 0055, generating a session secret and a first response corresponding to the challenge , based on the shared secret, authentication based on expected value from challenges value with shared secret), "an authenticating unit configured to produce an authentication result for said data transmitting apparatus based on the command authentication data in said response request command and said command expected value data when said response request command is received from said data transmitting apparatus" as (paragraph 0059, obtaining authentication information, the authentication information unit comprising a challenge and session secret to the mobile node identity and the random challenge and the shared data); and "a transmission unit configured to transmit a subsequent response message containing said response

authentication data to said data transmitting apparatus based on the authentication result by said authenticating unit" as (Fig 2, PAC sends authentication data to MT). **But Haverinen expressly fails to disclose** "a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message, and a judgment unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time; and the data receiving apparatus configured to receive data from the data transmitting apparatus.

However Rofheart discloses " a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message" as (Fig 7, compute round Trip time from transmitter to receiver), and "a judgment unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time" as (column 4, line 1-5, line 22-35, data transmission is determined based on authentication and response); and "the data receiving apparatus configured to receive data from the data transmitting apparatus" as (Fig 1A, Receiver received data from transmitter),

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission to a trusted third party.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a

device authentication with response time that taught by Rofheart because it would provide secure enablement communication with a specific subscriber .

Examiner Notes

11. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

13. Ishiguro et al (US 2002/0194475) discloses An information processing apparatus and an information processing method are capable of preventing information from being copied illegally.

14. Kudo et al (US 20040268131) discloses the content transmitting device and the content receiving device mutually authenticate each other to verify that the other device

respects copyright and rightfully handles content, and then content is encrypted by shared key data and transmitted.

15. Zuccheroto (US 6952771) discloses A system and method stores inquiry data, such as data representing questions or forms containing questions, to facilitate entry of shared authentication data for initialization.

16. Euchner (US7266682) discloses Data from a transmitter is extended to include authentication data on the application level by an application protocol. The authentication data is used by the receiver to determine whether the transmitter is known by the receiver.

17. Scherzer et al (US 6697644) discloses the invention provides optimization of communication links by using a control loop with a relatively long time constant and adjusting particular communication links based upon feedback from a virtual communication unit associated with a communication link.

18. Knight et al (US 6377589) discloses a communications system includes a telecommunications link (3) between a remote terminal (CPa-c) (such as a burglar alarm control panel) and a control station (1). Polling requests are transmitted on a digital messaging channel which is carried by the telecommunications link.

19. Willy (US 2003/0065918) discloses a method for establishing a link key between correspondents in a public key cryptographic scheme, one of the correspondents being an authenticating device and the other being an authenticated device.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abu Sholeman whose telephone number is (571)270-

7314. The examiner can normally be reached on Monday through Thursday 7:30 AM -

February 2, 2009, 2008

Abu Sholeman
Examiner
Art unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.